

JD:VTN
F.#2017R02166

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF
ONE BLACK ZTE CELLULAR DEVICE,
MODEL Z998BL, SERIAL NUMBER
32F4757800FD AND ONE BLACK
YELLOW BLU CELLULAR DEVICE,
MODEL STUDIO G2, SERIAL NUMBER
3070013017010497

APPLICATION FOR A SEARCH
WARRANT FOR ELECTRONIC
DEVICES

Case No. **18 M 0275**

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Michael Yun, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—two electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations (“HSI”) and have been for approximately one year. Prior to that, I was a criminal investigator for approximately four years at the New York State Tax Department and for two years at the New York State Attorney General’s Office. I have been involved in the investigation of numerous cases involving narcotics smuggling and trafficking. As a result of my training and experience, I am familiar with the

practice of searching for and obtaining electronic evidence to help identify, locate and prosecute defendants. I have participated in approximately thirty investigations involving search warrants, including warrants for the search of electronic devices.

3. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from my personal participation in this investigation and reports by other law enforcement authorities. When I rely on statements made by others, such statements are set forth only in part and in substance unless otherwise indicated.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Based on the facts set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence and instrumentalities of importation of cocaine, in violation of Title 21, United States Code, Sections 952(a), 960(a)(1) and 960(b)(2)(B)(ii), and possession of cocaine with intent to distribute, in violation of Title 21, United States Code, Sections 841(a)(1) and 841(b)(1)(B)(ii)(II).

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

5. The property to be searched is one black ZTE cellular device, model Z998BL, serial number 32F4757800FD and one Black Yellow BLU cellular device, model Studio G2, serial number 3070013017010497, hereinafter the "Devices." The Devices are currently in the custody of HSI within the Eastern District of New York.

6. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. On December 5, 2017, Lakisha Burton arrived at John F. Kennedy International Airport ("JFK Airport") in Queens, New York, aboard JetBlue Airways flight number B6 1818 from Port of Spain, Trinidad & Tobago. Upon her arrival at JFK Airport, Burton was stopped by agents of United States Customs and Border Protection ("CBP") at a control point near the baggage claim area. Burton had one checked bag and one carry-on bag.

8. Upon inspection of Burton's checked bag, CBP officers noticed that one side was unusually thick and heavy; the suitcase was probed, revealing a white powdery substance, which field-tested positive for cocaine. During inspection of Burton's carry-on bag, CBP officers noticed that one side was unusually thick and heavy. The carry-on bag was probed, revealing a white powdery substance, which also field-tested positive for cocaine. A total gross weight of the cocaine recovered from both bags was approximately 4.1 kilograms of cocaine.

9. Burton informed CBP that during her trip to Trinidad and Tobago, she stayed with an aunt for part of the time and at a hotel for the remainder of the time.

10. The records of JetBlue show that Burton arrived in Port of Spain on December 1, 2017 from JFK Airport and that the flight reservation for her travel to and from Port of Spain was made on November 22, 2017.

11. Burton was placed under arrest. CBP recovered the Devices from Burton and provided them to HSI once HSI responded to JFK Airport. The Devices are currently in the lawful possession of HSI and located within the Eastern District of New York.

12. Based on my education, training and experience, individuals involved in narcotics trafficking and individuals acting as couriers for drugs in a manner similar to Burton typically work in concert with others. Narcotics traffickers typically communicate with coconspirators about the scheme using their mobile electronic devices, including through telephone calls, text messages, electronic mails and instant messaging applications.

13. Based on the statements made by Burton to CBP, a search of the Devices could reasonably be expected reveal the name and contact information of Burton's aunt, information about Burton's hotel stay, information relating to the purpose of Burton's trip to Trinidad and Tobago, and other information that would assist in identifying and locating possible coconspirators of Burton's narcotics trafficking. Moreover, a search of the Devices could reasonably be expected to reveal information about how Burton paid for the expenses incurred during her trip. In my training and experience, I know that drug couriers often have flights and accommodations book or paid for by third parties and coconspirators.

14. In my training and experience, I know that the Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the HSI.

TECHNICAL TERMS

15. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global

positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital

data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

16. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media

player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

17. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

18. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

19. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques,

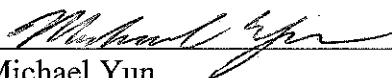
including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

20. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

21. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



Michael Yun
Special Agent
Department of Homeland Security,
Homeland Security Investigations

Subscribed and sworn to before me
on March 30, 2018:



THE HONORABLE
UNITED STATES
EASTERN DISTRICT OF


S. Pollak

AK
IE

ATTACHMENT A

The property to be searched is one black ZTE cellular device, model Z998BL, serial number 32F4757800FD and one Black Yellow BLU cellular device, model Studio G2, serial number 3070013017010497, hereinafter the "Devices." The Devices are currently in the custody of HSI within the Eastern District of New York.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of Title 18, United States Code, Sections 1951, 924(c)(1)(A)(i), 924(c)(1)(A)(ii) and 924(c)(1)(A)(iii) and involve Lakisha Burton and her co-conspirator(s) since December 1, 2017, including:

- a. all records and information on the Devices, including names and telephone numbers, as well as the contents of all call logs, text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, Facebook or other social media posts or messages, Internet activity (including browser history, web page logs and search terms entered by the user), and other electronic media constituting evidence, fruits or instrumentalities of the above-listed offenses;
- b. all contact lists;
- c. any information recording the whereabouts of Lakisha Burton and her co-conspirator(s) on or between November 1, 2017 and December 5, 2017;
- d. all bank records, checks, credit card bills, account information, and other financial records from on or after November 1, 2017;
- e. passwords, encryption keys and other access devices that may be necessary to access the Devices; and

- f. contextual information necessary to understand the evidence described in this attachment.

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.